

Konzepte von Betriebssystem-Komponenten:

SSH

Benutzersicht - Algorithmen - Administration

Andre Lammel <andre.lammel@gmx.de>

Konzepte von Betriebssystem-Komponenten:

SSH

Inhalt

Allgemeines

- Einführung
- Historisches
- Überblick

Anatomie

- Struktur
- Transport Layer
- Authentication Layer
- Connection Layer

Administration

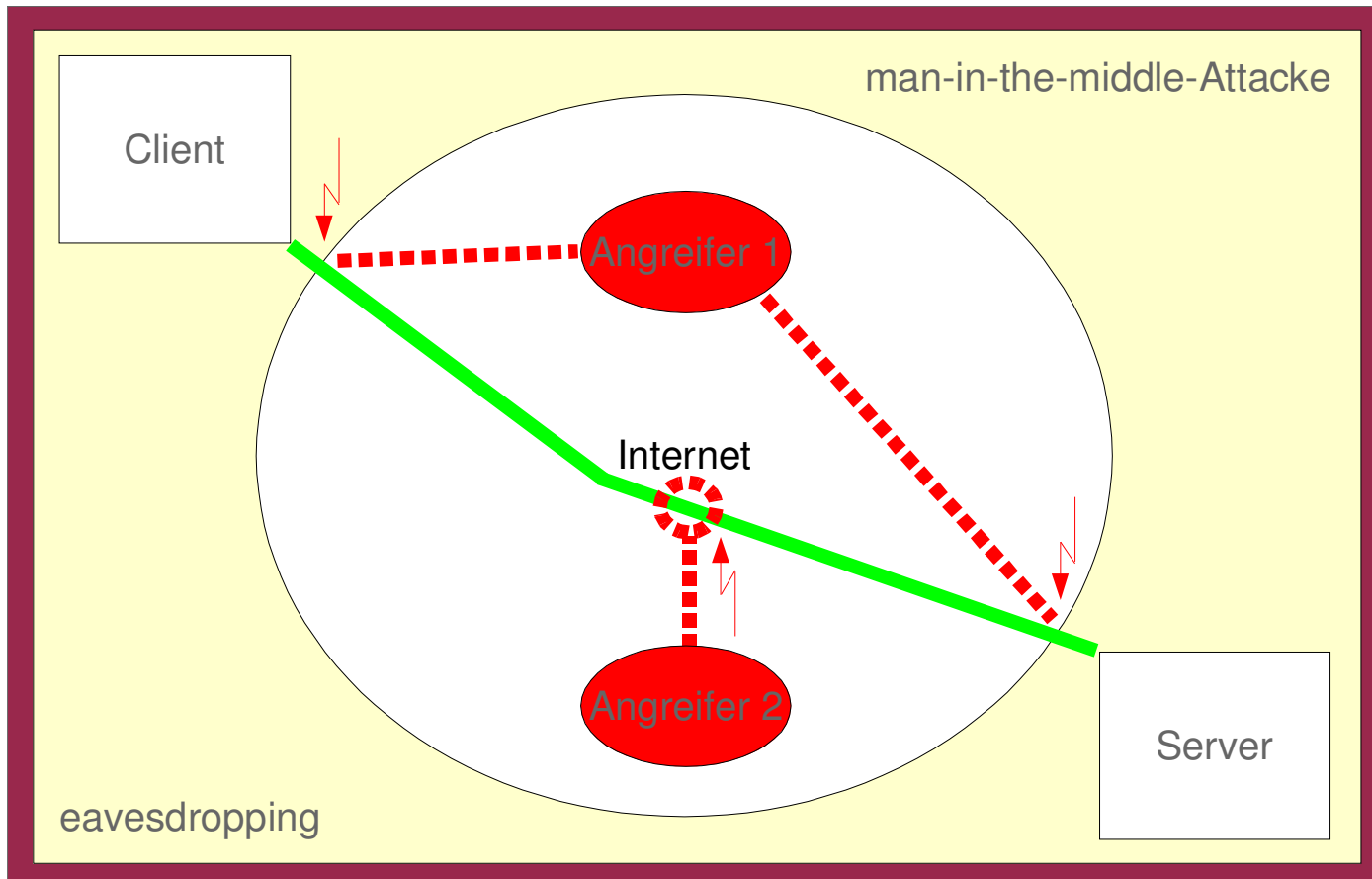
- Installation und Konfiguration
- Keys
- Sicherheit
- Fazit

Konzepte von Betriebssystem-Komponenten:

SSH

Allgemeines

Einführung



Konzepte von Betriebssystem-Komponenten:

SSH

Allgemeines

Historisches

1995 : Erstes Internet Draft von Tatu Ylönen zu SSH1

1999 : Das OpenBSD Projekt entwickelt OpenSSH
aus SSH 1.2.12

1999 : OpenSSH 1.2.2 erscheint mit OpenBSD 2.6
(SSH1)

2000 : SSH 2.0 mit OpenBSD 2.7
(SSH1 / SSH2)

Wichtigste Implementierungen des SSH-Protokolls:

- SSH von SSH Communications Security, Inc
- OpenSSH vom OpenBSD Projekt.

Konzepte von Betriebssystem-Komponenten:

SSH

Allgemeines

Überblick

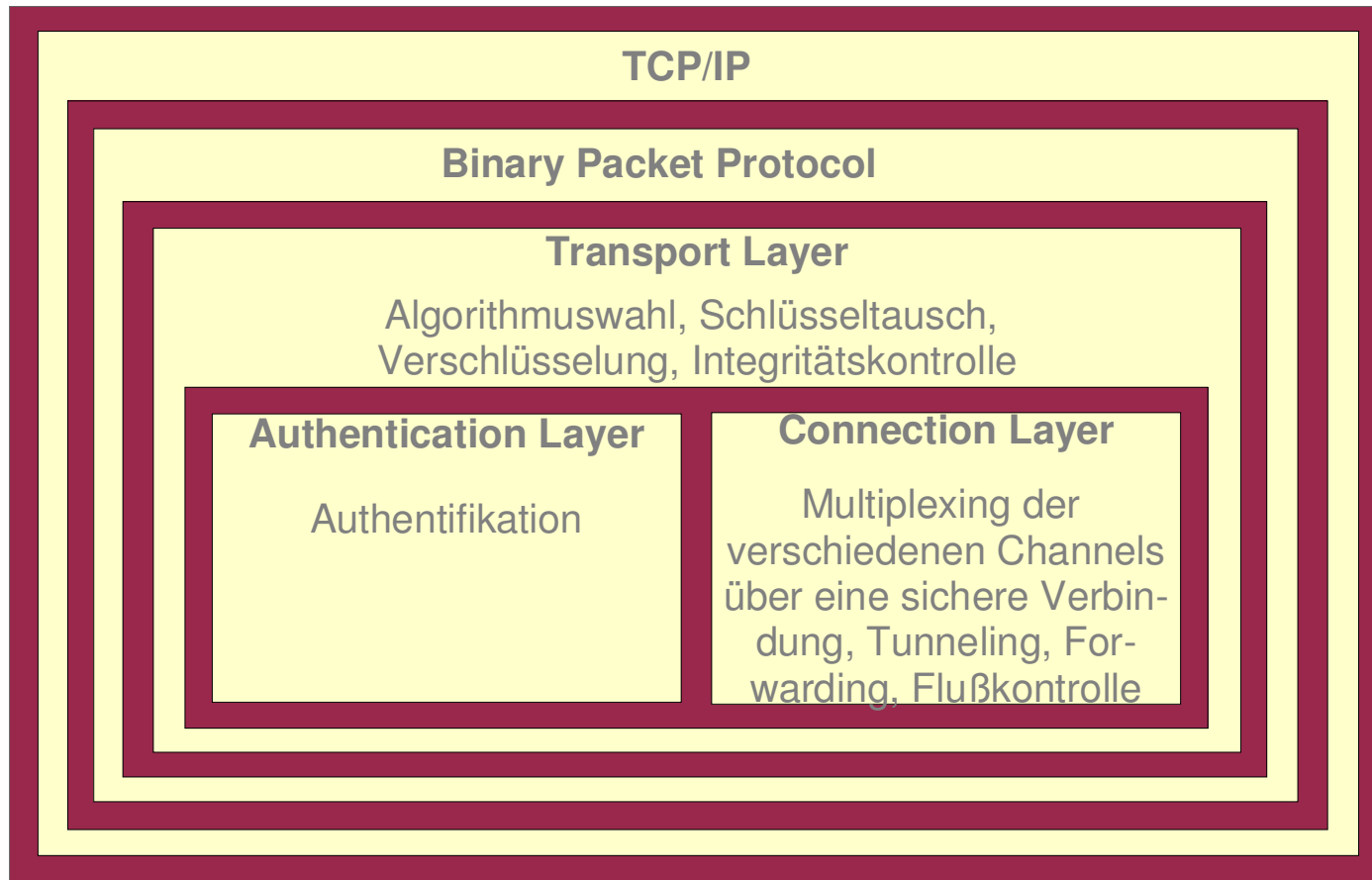


Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Struktur



Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer I - Binary Packet Protocol

<i>Name</i>	<i>Beschreibung</i>
packet_length (pl)	Paketlänge ohne Felder packet_length und mac
padding_length (fl)	Länge der Fülldaten
payload (p)	Nutzbarer Inhalt des Paketes
padding (f)	Fülldaten
mac (m)	Message Authentication Code (MAC)

$n \in \mathbb{Z}$

c = cipher block size des verwendeten Verschlüsselungsalgorithmus

$pl = \text{length}(pl) + \text{length}(fl) + \text{length}(p) + \text{length}(f) = n \cdot \max(8, c)$

Limitierungen:

$pl_{\min} = \max(16, c) + \text{length}(mac)$

$fl_{\max} = 32768$ Byte unkomprimiert

$pl_{\max} = 35000$ Byte, größere Pakete nach Vereinbarung

Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer II - Diffie-Hellman-Algorithmus

$g = 1$ für diffie-hellman-sha1
 p = sehr große, bekannte Primzahl
 $X, Y \in \{ 1, p - 1 \}$, Zufallszahlen

allgemein muß g folgende Bedingung erfüllen:

$g \in \mathbb{Z}$, $g < p$
für alle $n \in \{ 1, p - 1 \}$ existiert eine Potenz K von g , so daß $n = g^K \pmod p$
weiterhin sollte $(n - 1) / 2$ ebenfalls eine Primzahl sein. Mit

$h_x = g^x \pmod p$
 $h_y = g^y \pmod p$

gilt dann, daß die Anwendung von h_y und h_x kommutativ ist:

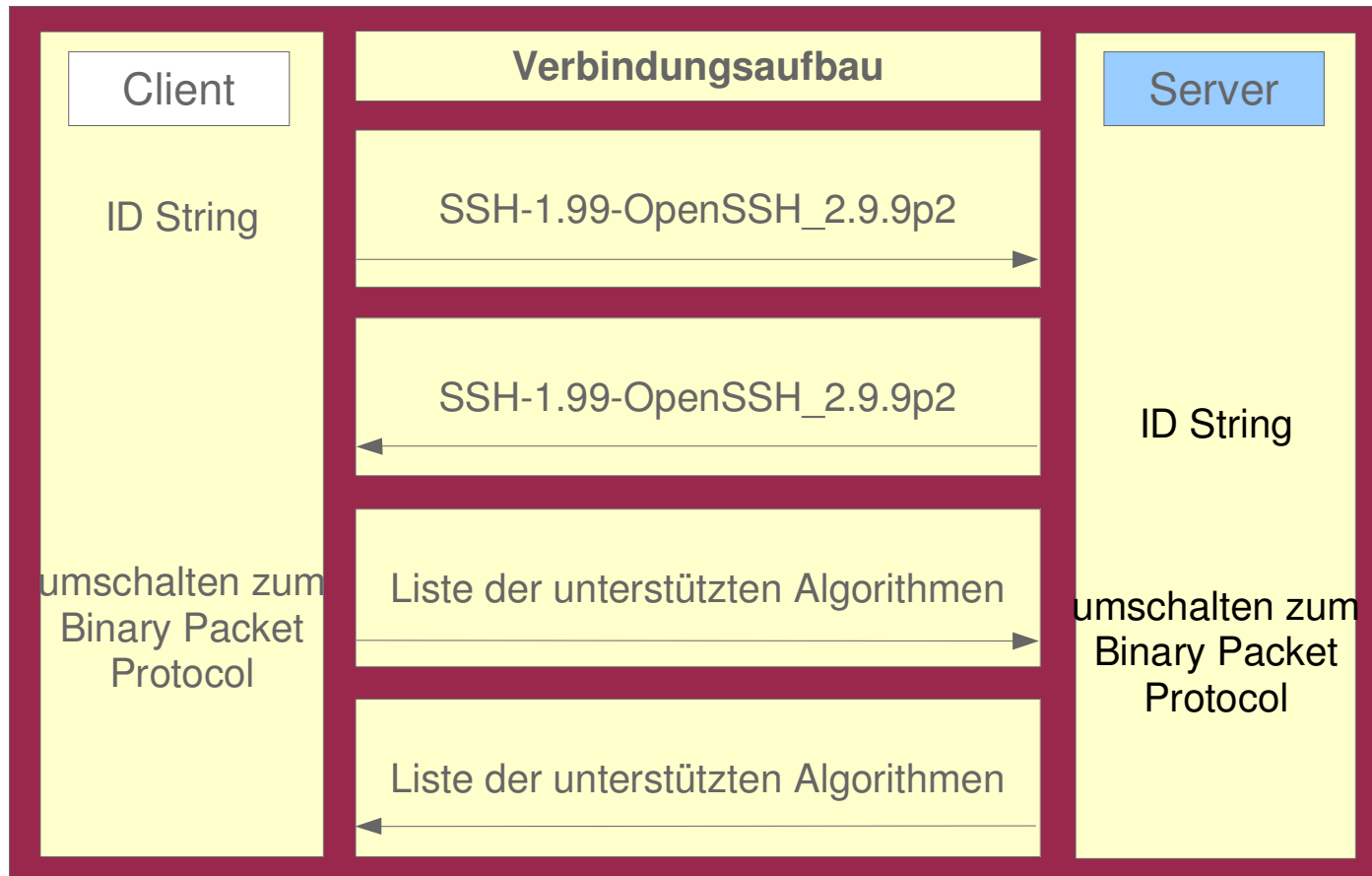
$$h_y(h_x(g)) = h_x(h_y(g))$$

Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer III - Kommunikation

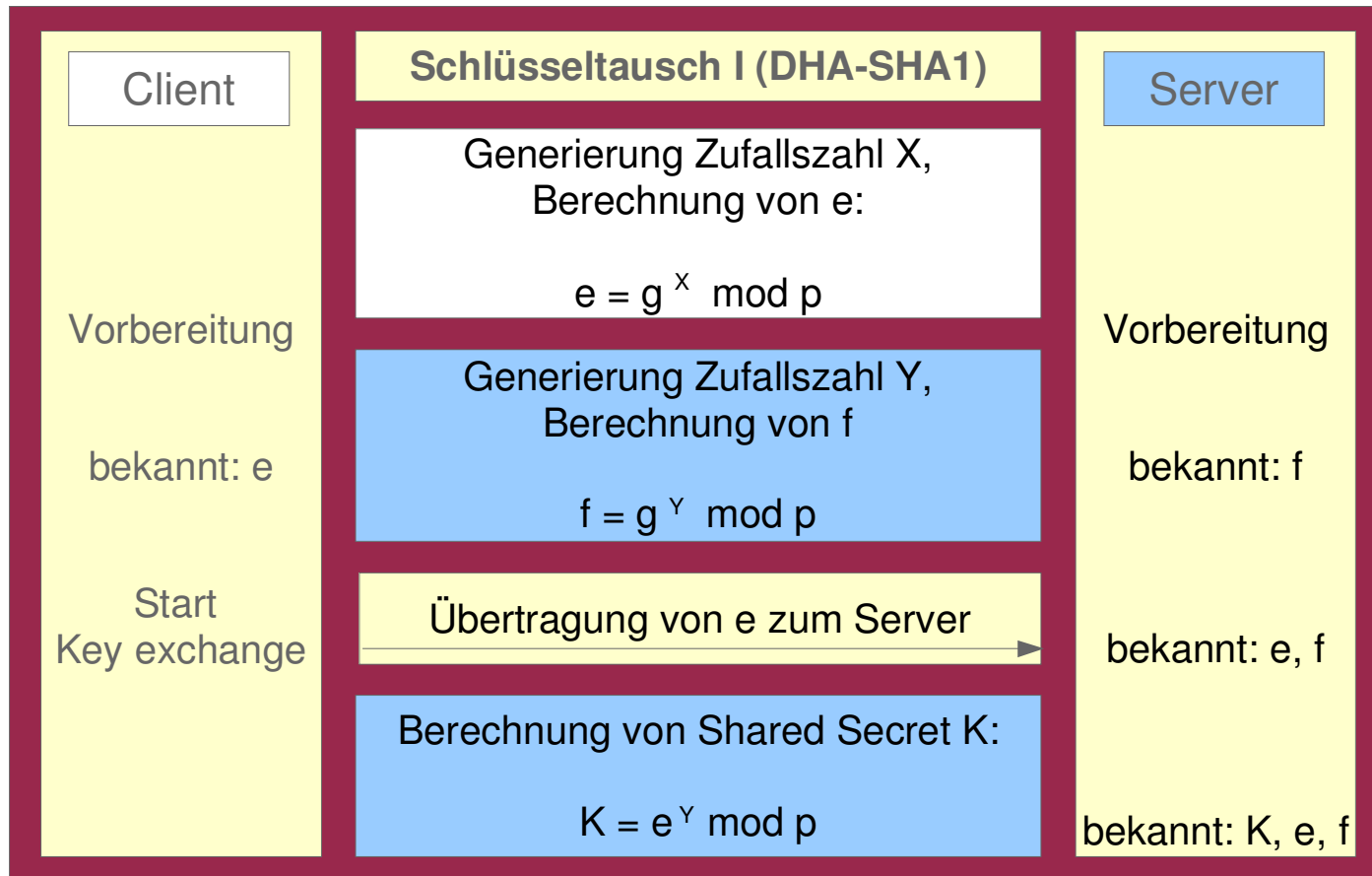


Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer IV - Kommunikation

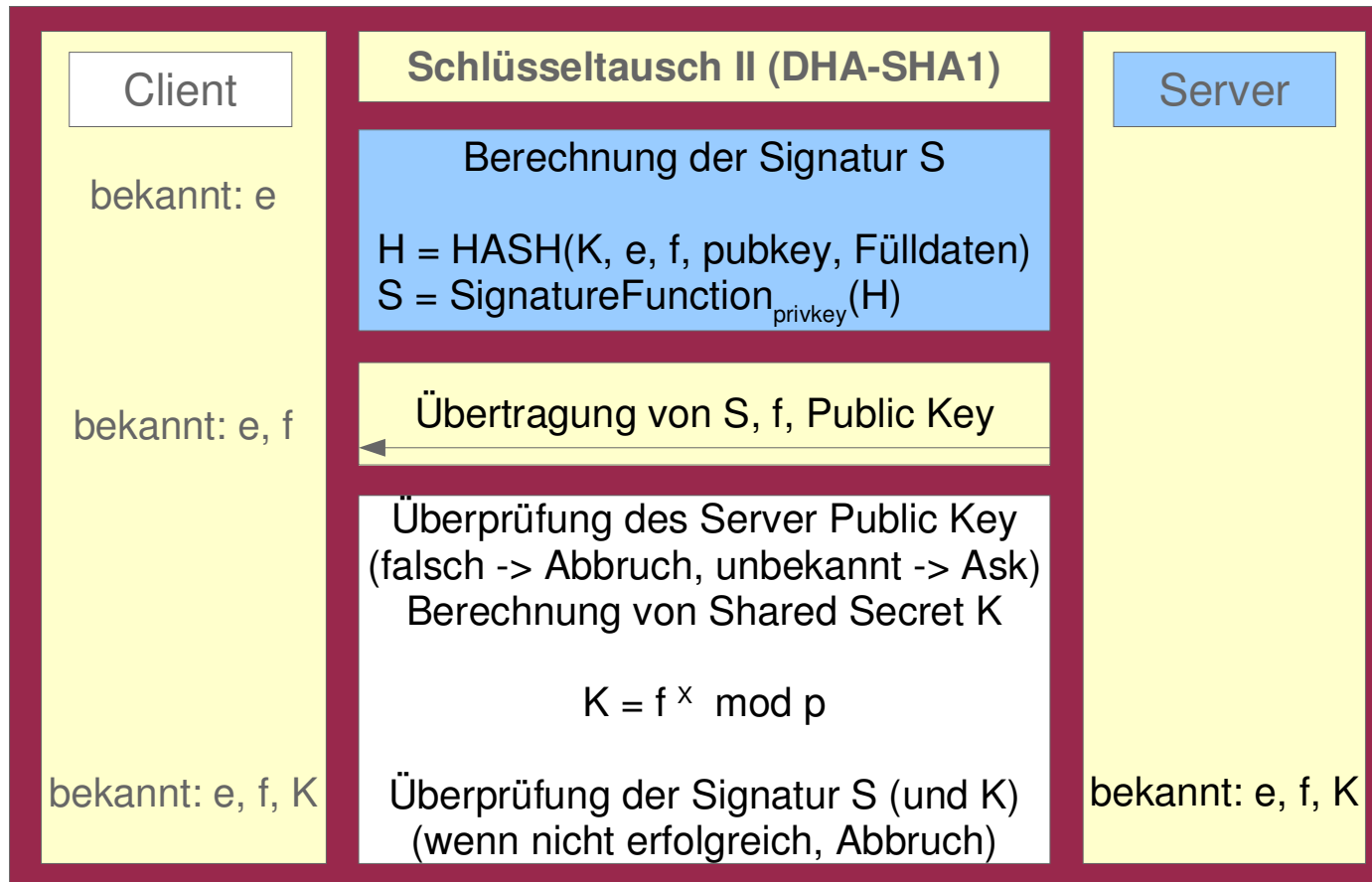


Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer V - Kommunikation

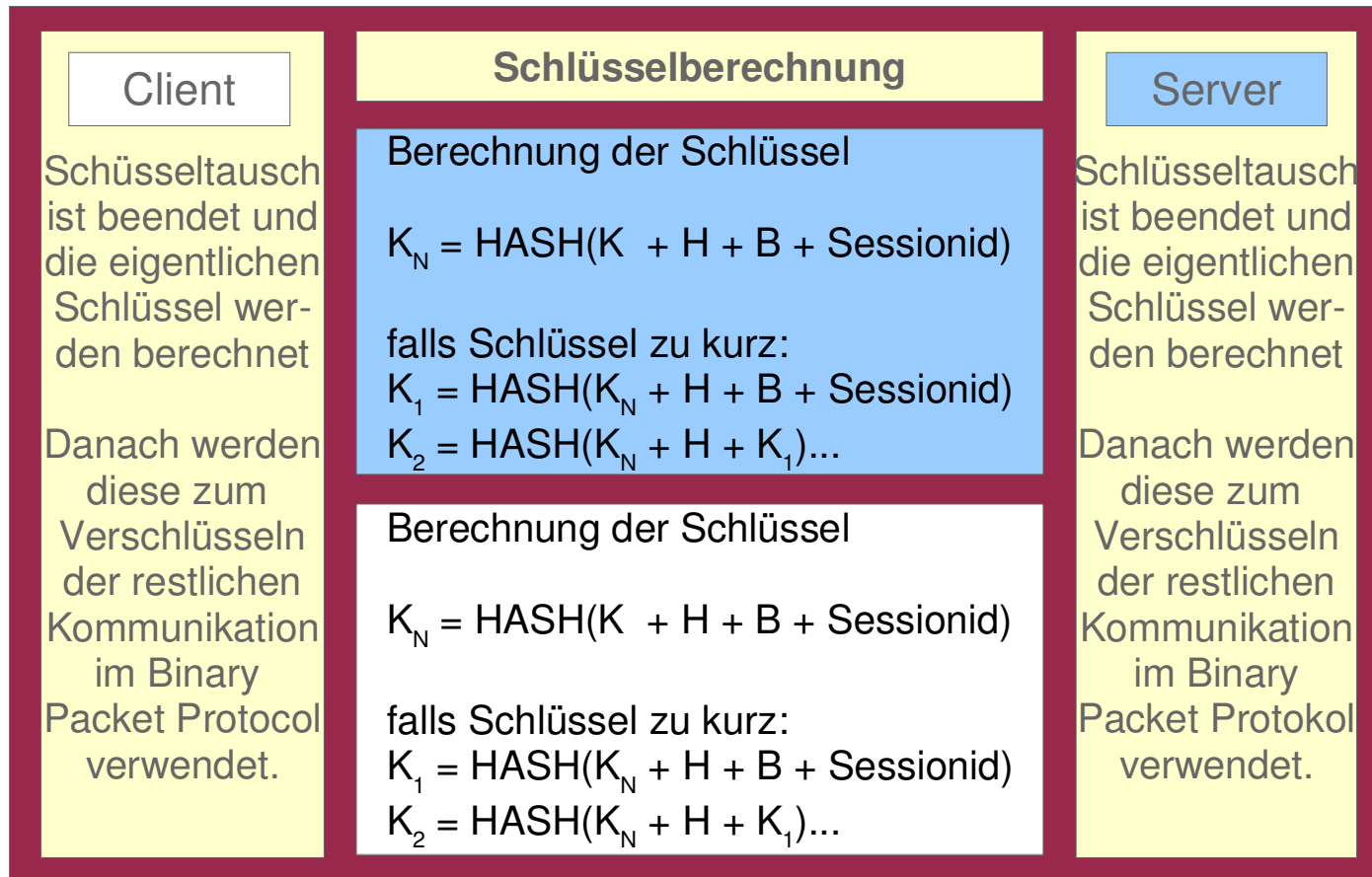


Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer VI - Kommunikation

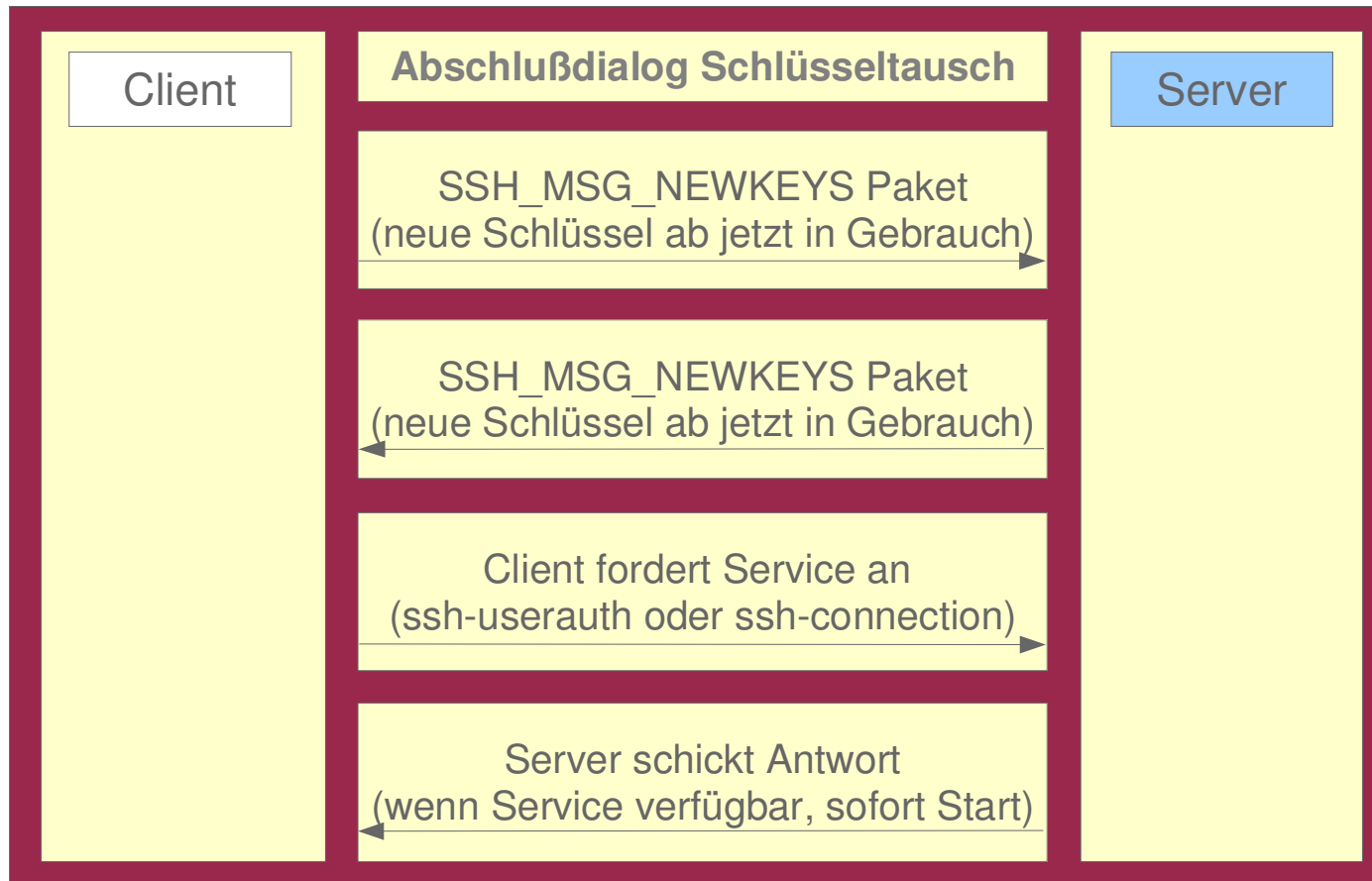


Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer VII - Kommunikation



Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer VIII - Verschlüsselung, MAC und Kompression

Typ	Name	Verschlüsselung	Komprimierung	MAC
uint32	packet_length (pl)	verhandelbar	nein	ja
byte	padding_length (fl)		nein	ja
byte[i]	payload (p)		verhandelbar	ja
byte[j]	padding (f)		nein	ja
byte[k]	mac (m)	nein	nein	nein

K = Shared Secret aus dem Schlüsseltausch
S = Sequence Number des Paketes (laufende Nummer)

mac = MACAlgorithmus(pl, fl, p, f, K, S)

Der MAC wird vor der Verschlüsselung, aber nach der Kompression berechnet. Der Client vergleicht den Wert seiner Berechnung mit dem empfangenen Wert. Unterschiedliche Werte bedeutet, daß die Daten unterwegs verändert wurden. Die Kompression erfolgt mit Zlib.

Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Transport Layer IX - Sicherheit

Allgemeine Sicherheitsrisiken:

- Aushandlung einer Verbindung ohne Verschlüsselung oder MAC
- Man-in-the-middle-Attacken (Überprüfung des Server Keys !)
- Allgemein bekannte Gefahren beim Diffie-Hellman Algorithmus
- Verwendung der Algorithmen im cipher block chaining (CBC) mode
- brute-force-Attacken auf den Verschlüsselungsalgorithmus

Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Authentication Layer I – Methoden

Public Key

Der Public Key des Benutzers wird zur Authentifizierung verwendet

Passwort

Der Benutzer authentifiziert sich mithilfe eines Passwortes, Wechsel des Passwortes ist während des Authentifizierungsvorganges möglich

Host based

Der Public Key des Client Rechners wird zur Authentifizierung genutzt

Alle Daten werden im Klartext übertragen, die Verschlüsselung und Integritätskontrolle erfolgt im darunterliegenden Transport Layer.

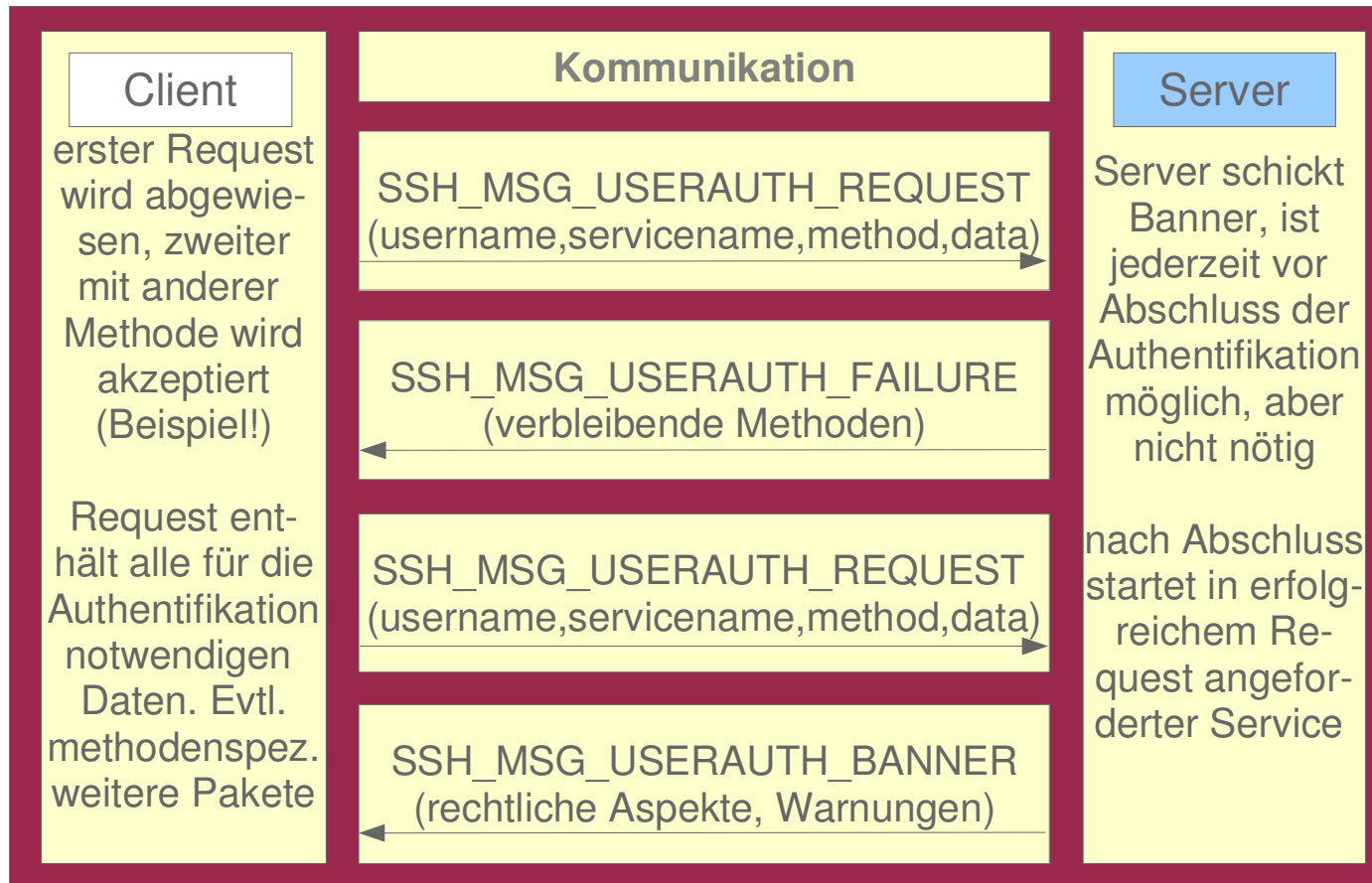
Die Authentifizierung durch Public Keys erfolgt mit dem im Transport Layer vereinbarten Algorithmus.

Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Authentication Layer II - Kommunikation

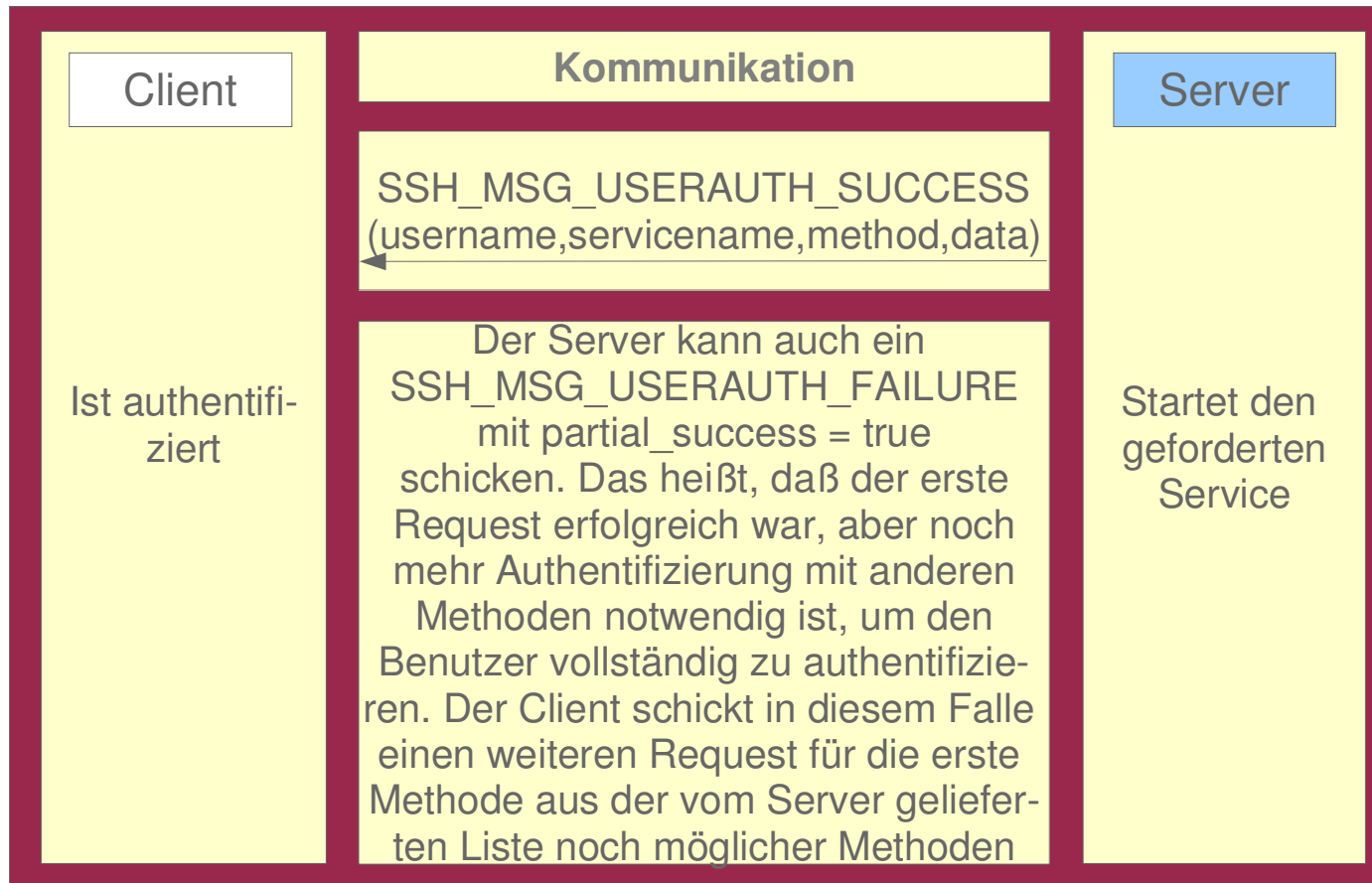


Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Authentication Layer III - Kommunikation



Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Authentication Layer IV – Sicherheit

<i>Methode</i>	<i>Sicherheit</i>	<i>Gefahren</i>
Public Key	sehr gut	zu kurze Schlüssel, unsichere Algorithmen
Passwort	mittel	Zu kurze oder einfache Passwörter
Hostbased	wenig	Private Host Key ungenügend geschützt

Allgemeine Sicherheitsrisiken:

- keine oder zu schwache Verschlüsselung im Transport Layer
- kein MAC im Transport Layer
- Konfigurationsfehler durch den Administrator
- Für alle Benutzer lesbare Private Keys / Public Keys
- fehlende Policies für erlaubte / unerlaubte Authentifizierungsmethoden
- unklare Rechtevergabe an die einzelnen Benutzer
- Kompromittierung der Clientsoftware
- SSH Keystroke Timing Attack bei der Passworteingabe
- Lokale Keyboard Sniffer

Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Connection Layer I – Begriffe

Channel

einzelner Kommunikationskanal innerhalb des Connection Layer innerhalb dessen der Datentransfer für eine bestimmte Funktionalität erfolgt

Channel Request

Nachricht zum Steuern eines Kommunikationskanales

Global Request

Nachricht zum Setzen globaler Parameter

Window Adjust Request

Nachricht zur Steuerung des Datenflusses

Magic Number

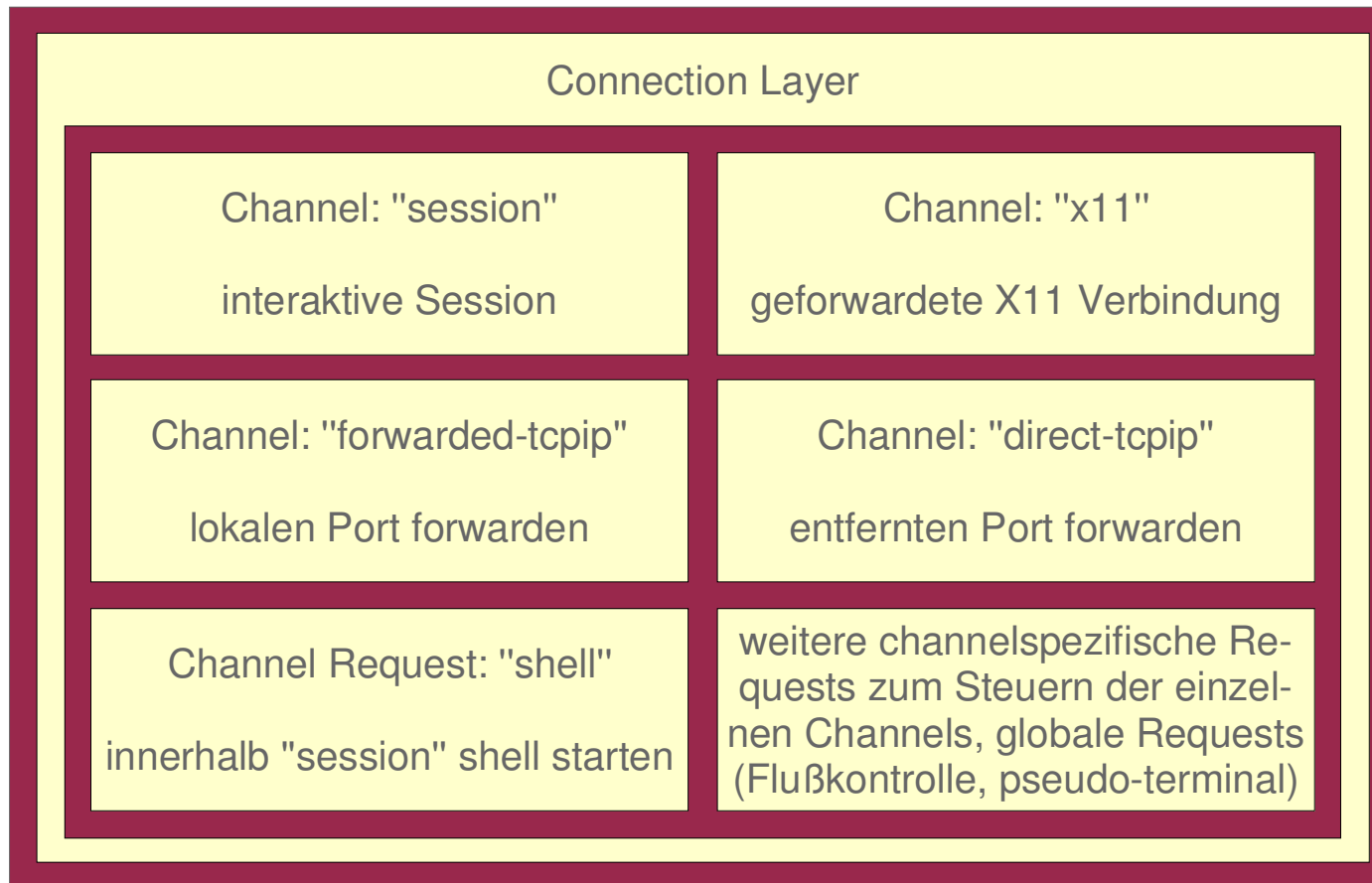
Eindeutige Nummer zur Identifikation eines Kommunikationskanales

Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Connection Layer II - Aufbau

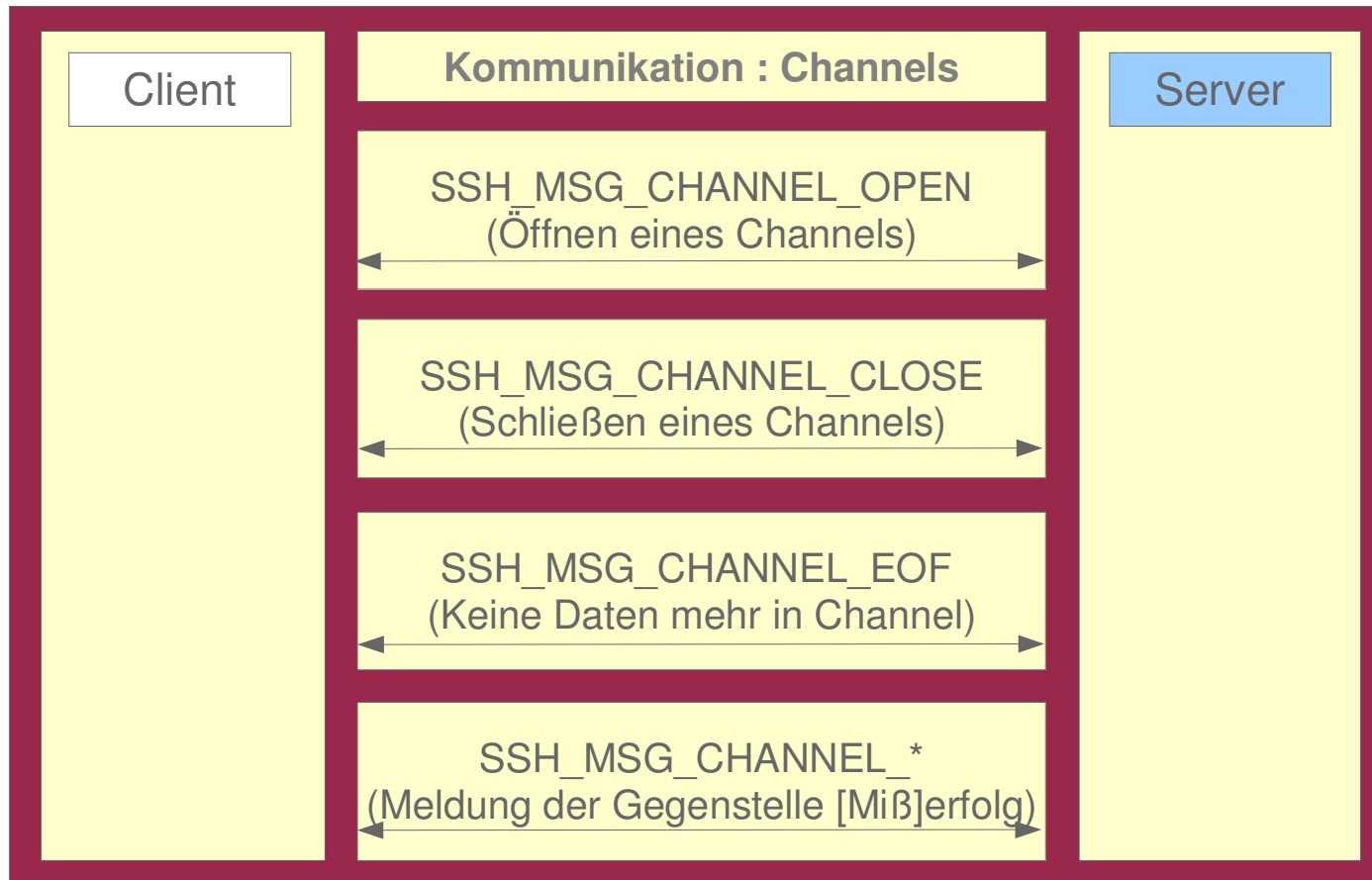


Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Connection Layer III - Kommunikation : Channels

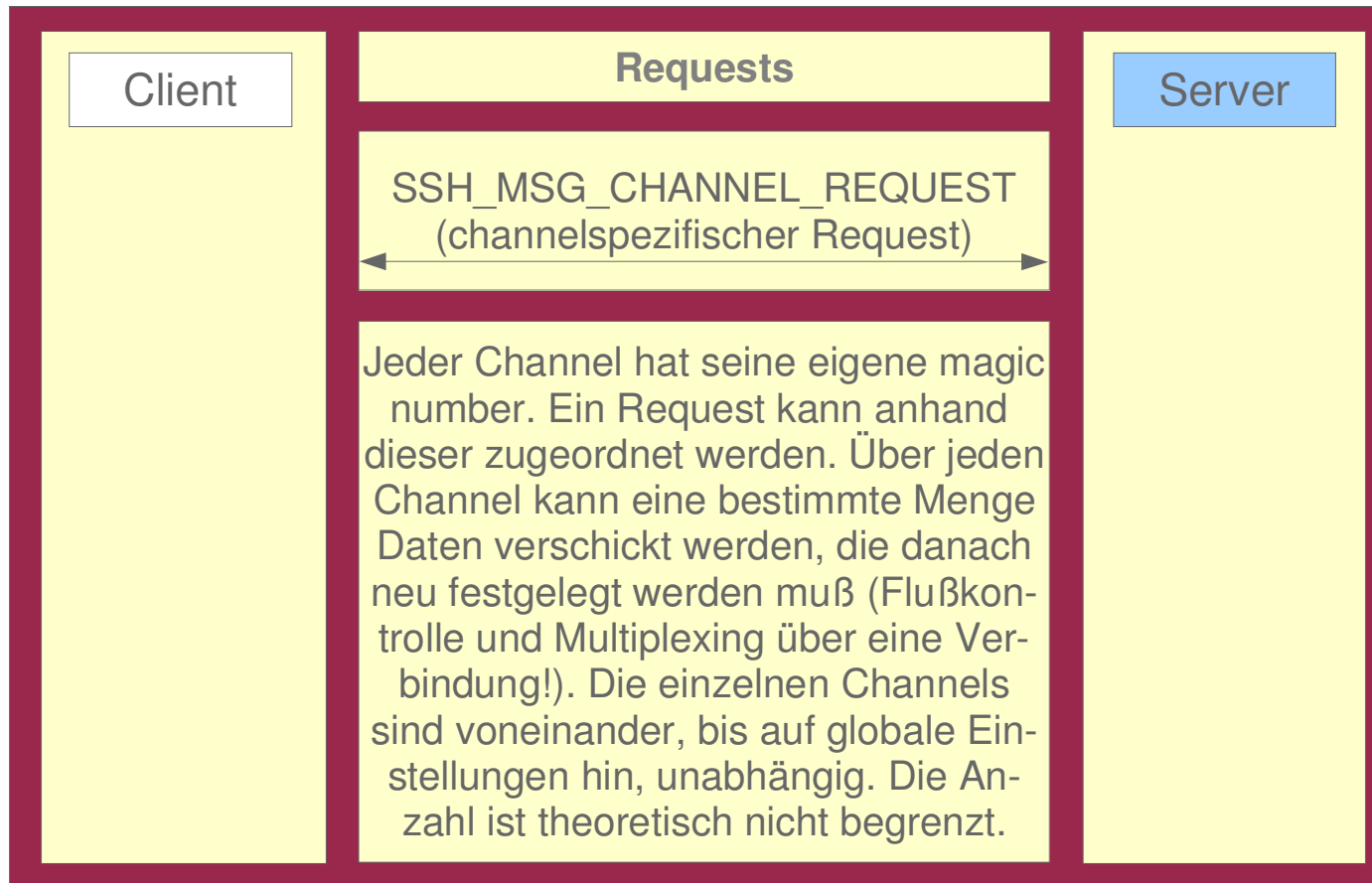


Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Connection Layer IV - Kommunikation : Requests



Konzepte von Betriebssystem-Komponenten:

SSH

Anatomie

Connection Layer V - Sicherheit

Allgemeine Sicherheitsrisiken:

- Umgehung von Firewalls über Forwardings (tcp/ip, x11)
- Umgehung von contentsensitiven IDS-Systemen
- Erlangung von Rechten (Konfigurationsfehler)
- Ausnutzung von Softwarefehlern (X11-Exploits)
- Erlangung einer Shell
- Setzen unerlaubter Environmentvariablen
- Ausnutzung der Remote Command Execution
- Auslesen geschützter Daten

Konzepte von Betriebssystem-Komponenten:

SSH

Administration

Installation und Konfiguration

Quellen:

- <http://www.openssh.com>
- <http://www.ssh.com>

Wichtige Tipps bei der Konfiguration:

- Kein X11 Forwarding
- Kein TCP/IP Forwarding
- Keine Hostbasierte Authentifikation
- Immer Passwort abfragen
- Besser nur Public Key Authentifikation
- Benutzer explizit festlegen
- Root für alle Funktionen sperren
- Nur verschlüsselte Kommunikation mit MAC erlauben
- Host Keys und Benutzer Keys mindestens 1024 Bit
- Passwortgeschützte Schlüssel für die Benutzer
- Verwendung von Protokollversion 2 erzwingen

Konzepte von Betriebssystem-Komponenten:

SSH

Administration

Keys

Unterstützte Schlüsselformate (RSA und DSA):

- ssh (implementierungseigenes Format)
- x509v3 (X.509 Version 3)
- spki (SPKI Zertifikate)
- pgp-sign (OpenPGP Zertifikate)

Empfohlene Schlüssellänge:

- length(KEY) \geq 1024 Bit

Empfohlenes Format:

- implementierungseigenes Format
- DSA Keys (RSA inzwischen gebrochen)

Konzepte von Betriebssystem-Komponenten:

SSH

Administration

Sicherheit

Sicherheitsrisiken im Überblick:

- man-in-the-middle-Attacken (Transport Layer)
- brute-force-Attacken (Transport Layer)
- Lokale Attacken (alle Layer)
- algorithmenspezifische Attacken
- Fehler in den einzelnen Implementierungen
- Konfigurationsfehler

Konzepte von Betriebssystem-Komponenten:

SSH

Administration

Fazit

Pluspunkte:

- SSH in der Version 2 bietet weitaus mehr Sicherheit als die Protokolle telnet, rsh, rcp, rlogin, etc.
- Datenintegrität und Verschlüsselung bieten Privatsphäre
- Das Protokoll ist offen und erweiterbar

Minuspunkte:

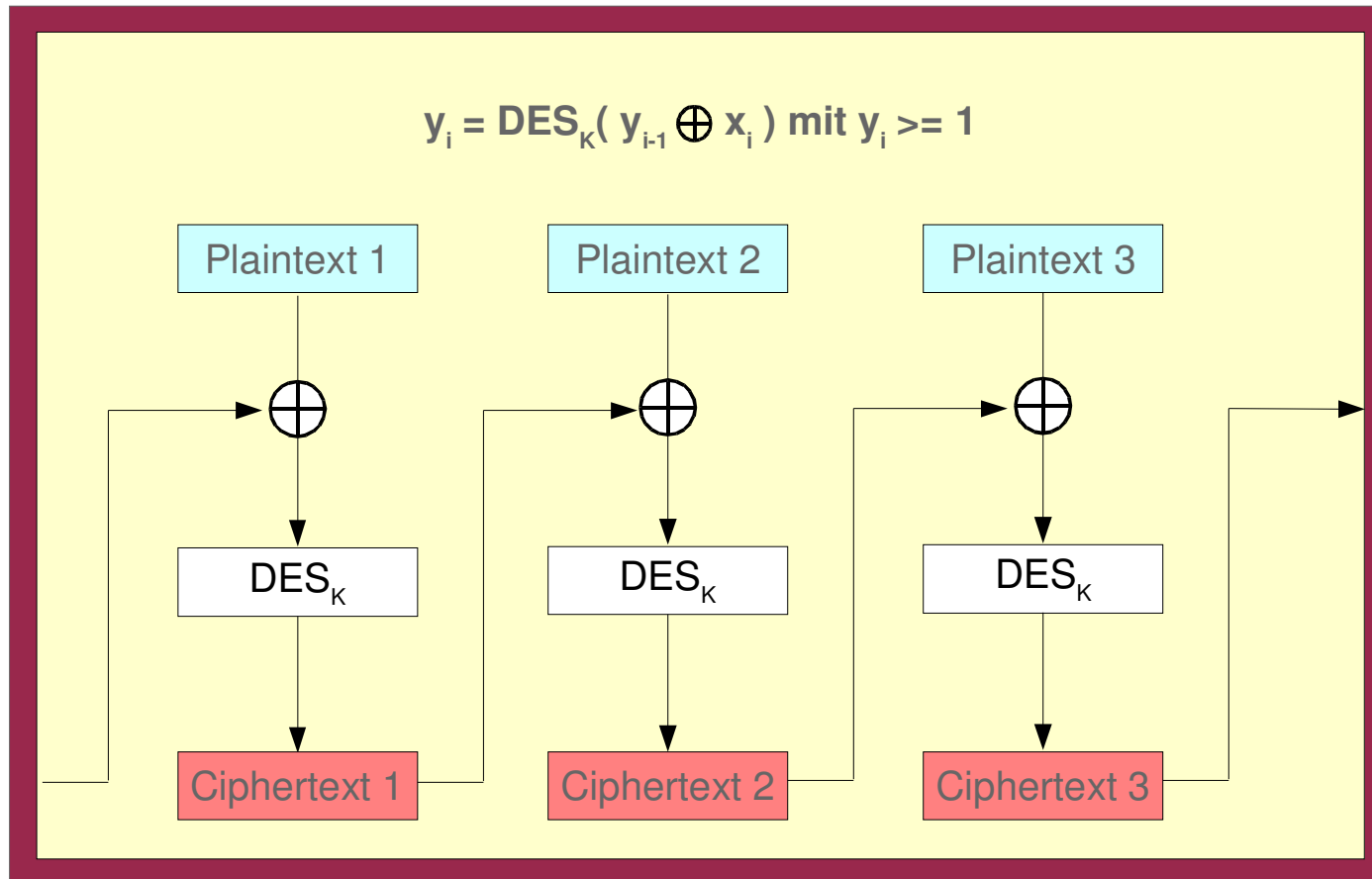
- Das Schlüsseltauschproblem besteht weiterhin
- Die verwendeten Algorithmen sind problematisch
- Die gesamte Sicherheit baut auf dem Transport Layer auf
- Darüberliegende Protokolle bieten keine Möglichkeit der Überprüfung der Kommunikation innerhalb des Transport Layers
- Durch die Verwendung von SSH entstehen neue Angriffsszenarien
- Die Sicherheit ist von der Implementierung und der Konfiguration abhängig

Konzepte von Betriebssystem-Komponenten:

SSH

Erklärungen

CBC (Cipher Block Chaining) Mode am Beispiel von DES



Konzepte von Betriebssystem-Komponenten:

SSH

Erklärungen

CBC (Cipher Block Chaining) Mode am Beispiel von DES

Eigenschaften des Cipher Block Chaining Mode:

- Änderung der Reihenfolge von Blöcken wird erkannt
- Löschung von Blöcken wird erkannt
- Übertragungsfehler wirken sich nur auf den aktuellen und den nachfolgenden Block aus
- Statistische Eigenschaften des Klartextes werden über alle Blöcke des Ciphertextes verstreut, was die Cryptoanalyse erschwert.